INTRODUKTION:

NIP (Nascom Inversassembler Package) er et disassembleringsprogram specielt designet til NASCOM 1/2 med NAS-SYS monitor og eventuelt NAP assembleren.

NIP disassemblerer Z-80 maskinkode til standard ZILOG/MOSTEK Z-80 mnemonics, og kan, hvis man ønsker det, sætte labels i det disassmeblerede program.

Ud over at udskrive den disassmeblerede tekst på skærm og/eller printer, kan NIP også gemme den i NAP assemblerens kildetekstbuffer. På denne måde bliver der mulighed for at relokere/editere maskinkodeprogrammer, uden at man er i besiddelse af den originale kildetekst.

NIP er også i stand til at disassemblere et program der er flyttet bort fra sin normale eksekveringsadresse. Således undgås det problem, der ellers ville opstå, når et program ligger på samme sted i lageret som NIP.

NIP ASSEMBLERSYNTAX:

NIP's assemblersyntax er fuldstændig kompatibel med NAP assembleren og kan direkte oversættes af denne. Sammenlignet med ZILOG/MOSTEK Z-80 assembler bør følgende iagttages:

* Alle labels bliver efterfulgt af et kolon når de defineres.

* Pseudoinstruktionen DB benyttes i stedet for DEFB og DEFM til at definere en enkelt byte eller en string i lageret.

* Pseudoinstruktionen DW benyttes i stedet for DEFW til at definere en adresse i lageret.

* Instruktionerne RST 10H (D7H) og RST 18H (DFH) bliver oversat til henholdsvis RCAL $+disp (hvor disp er det relative offset til den subrutine der skal kaldes) og SCAL nn (hvor nn er nummeret på den subrutine i NAS-SYS der skal kaldes). De bytes der efterfølger en RST 28H instruktion bliver oversat som stringdata (se "A" kommandoen), indtil et 0 mødes. Disse instruktioner er ikke standard i Z-80 assembleren og kræver, at systemet benytter NAS-SYS eller en anden monitor med tilsvarende funktioner.

NIP INDLÆSNING OG OPSTART:

NIP leveres på et kassettebånd der er udlæst med NAS-SYS "W" kommando på 300 baud. Hvis det første indlæsningsforsøg fejler er der en anden udlæsning på den anden side af båndet. NIP koldstartes ved at indtaste:

E2000 <enter> (EC400 for ROM versionen)

Ved en koldstart nulstilles alle options og dataområdebufferen slettes (se herom senere). NIP kan vermstartes ved at indtaste:

E2003 <enter> (EC402 for ROM versionen)

NIP BETJENING:

Når NIP er opstartet som beskrevet ovenfor udskrives der en højrepil på skærmen for at indikere, at programmet venter på input.

Alle NIP kommandoer består, i lighed med NAS-SYS, af et enkelt bogstav.

NIP KOMMANDOER:

A xxxx yyyy z DEFINER DATAOMRÅDE

Ved hjælp af denne kommando defineres et område inden for hvilket der er data og ikke instruktioner. Når NIP disassemblerer imellem xxxx og yyyy, bliver de enkelte bytes udskrevet i et format der afhænger af z:

z=0: Bytedata. Alle bytes inden for dette område bliver udskrevet som en DB instruktion efterfulgt af de relevante tal.
z=1: Stringdata. Hvis det er muligt bliver en byte udskrevet som en del af en tekststreng; hvis ikke er formatet som ved z=0.
z=2: Adressedata. Databytes bliver udskrevet som adresser, dvs. en DW instruktion efterfulgt af to bytes der angiver adressen.

Op til 48 dataområder kan defineres.

B xxxx yyyy NAP TEKSTBUFFER ADRESSER

Denne kommando definerer NAP tekstbufferens start- og slutadresser (de samme som specificeres når NAP koldstartes). Denne kommando bør benyttes inden "N" kommandoen, hvis NAP ikke er blevet koldstartet forinden.

C+ COMMENTS ON

Når commentfunktionen er on, bliver der sat comments i programmet svarende til ASCII værdien af instruktionen. Hvis ASCII værdien er et kontroltegn (mellem 0 og 31), bliver der udskrevet et punktum i stedet.

C- COMMENTS OFF

Fjerner commentfunktionen.

D xxxx yyyy zz DISASSEMBLERING

Disassemblerer fra xxxx til yyyy og stopper hvergang der er udskrevet zz linier. Hvis man trykker ESC her, går NIP tilbage til inputmode; ellers udskrives der endnu zz linier.

E SLET DATAOMRÅDE ADRESSER

Denne kommando sletter alle de dataområde adresser, der er indtastet med "A" kommandoen.

F xxxx yyyy .. FIND SØGESTRENG

Denne kommando undersøger lageret mellem xxxx og yyyy, og udskriver alle de adresser hvor den indtastede søgestreng forekommer. En søgestreng kan være op til otte bytes lang. En byte kan enten indtastes som et hextal eller som ASCII. I det sidste tilfælde skal karakteren stå efter et komma. Et spørgsmålstegn (?) i stedet for en af de to ovenstående muligheder indikerer at denne byte kan være hvad som helst. For eksempel vil kommandoen "F 1000 2000 3A ? ? FE ,0" udskrive adresserne på alle de steder i lageret mellem 1000H og 2000H, hvor A-registret bliver loadet indirekte fra en adresse og derefter sammenlignes med et ASCII 0.

H+ HEXNOTATION ON

Når hexnotation er on bliver alle bytes (dvs. 8-bits tal) udskrevet i hexadecimal notation (undtaget er dog relative offsets og portnumre der altid bliver udskrevet i decimal notation).

H- HEXNOTATION OFF

Når hexnotation er off bliver alle bytes udskrevet i decimal notation.

J xxxx DISASSEMBLERING MED JUMPTEST

Denne kommando disassemblerer og udskriver fra adressen xxxx, indtil en af de følgende instruktioner mødes:

JP nnnn	JR $+disp	RET
JP (HL)	JP (IX)	JP (IY)
HALT	SCAL 5BH	

Når dette sker stopper NIP og venter på et input. Hvis man trykker ESC, går programmet tilbage til inputmode; ellers fortsættes der, til en af de ovenstående kommandoer igen mødes.
"J" kommandoen er især anvendelig, når man skal bestemme hvor et maskinkodeprogram slutter, idet en af de ovennævnte instruktioner normalt er den sidste i et program.
Labelfunktionen virker ikke ved "J" kommandoen.

L+ LABLES ON

Når labelfunktionen er on, bliver der sat labels i det disassemblerede program. Dette foregår ved, at NIP disassemblerer i to gennemløb. I det første bliver alle adresserefe-rancer gemt på symbolstacken. Hvis en af disse adresser mødes i andet gennemløb, bliver der sat en label på det pågældende sted. De adresser (labels), der ligger på symbolstacken, men som ikke bliver mødt i andet gennemløb bliver defineret ved hjælp af EQU instruktioner til sidst i programmet.
Hvis symbolstackens start- og slutadresse ikke er defineret (ved hjælp af "S" kommandoen), virker labelfunktionen ikke.

L- LABELS OFF

Fjerner labelfunktionen.

N xxxx yyyy DISASSEMBLER TIL NAP

Når denne kommando bruges, bliver det disassemblerede program (fra xxxx til yyyy) gemt i NAP assemblerens kildetekstbuffer. Hvis NAP ikke er i systemet, bør denne kommando undgås. Hvis NAP ikke er blevet koldstartet, skal "B" kommandoen bruges inden "N" kommandoen kaldes.

O xxxx yyyy DEFINER OFFSET

Hvis det program der skal disassembleres ikke ligger på det sted hvor det normalt eksekveres, bruges "O" kommandoen. Hvis for eksempel et program normalt starter i 2000H men nu er flyttet, så det starter i 5000H, vil kommandoen O 2000 5000 fortælle NIP at instruktionerne skal hentes fra 5000H og op, men disassembleres, som om de lå fra 2000H og op.
Grunden til, at der skal skrives to adresser, er, at man ikke selv behøver at regne offsettet ud. I ovennævnte tilfælde kunne man således godt have skrevet O 0 3000, idet yyyy-xxxx giver det samme.
Når offsettet er defineret, kan de efterfølgende kommandoer indtastes, som om programmet lå i xxxx.
Kommandoen O 0 0 nulstiller offsetfunktionen.

Q QUIT

Quit kommandoen returnerer til NAS-SYS.

R+ PCR-FUNKTION ON

Når PCR-funktionen (Program Counter Relative) er on bliver operanden ved relative hop (JR) og relative kald (RCAL) udskrevet som $+disp. For eksempel vil instruktionen 20 05 blive disassembleret til JR NZ,$+7.

R- PCR-FUNKTION OFF

Når PCR-funktionen er off bliver operanden ved relative hop og kald udskrevet som den absolutte adresse.

S xxxx yyyy SYMBOLSTACK ADRESSER

Denne kommando fortæller NIP hvilket lagerområde, den må bruge som symbolstack når labelfunktionen er i brug.
Da princippet er som en almindelig stack (hvilket vil sige at adresserne bliver skubbet på symbolstacken startende fra yyyy og nedad mod xxxx), kan man med fordel bruge den øverste del af RAM lageret til symbolstacken.
Hvis labelfunktionen ikke bruges, er det heller ikke nødvendigt at definere symbolstackens adresser, idet den slet ikke kommer i brug.

T xxxx yyyy zz TABULER

Tabuler kommandoen er med som en udvidelse af NAS-SYS "T" kommando, idet den udover at udskrive den hexadecimale værdi af hver byte tillige udskriver ASCII værdien (på samme måde som commentfunktionen). Dette er især anvendeligt, når man skal bestemme hvilke områder af et maskinkodeprogram, der er tekst (data).
Det ved "O" kommandoen definerede offset berører, i lighed med "A","D","F" og "J" kommandoerne, også "T" kommandoen.

U+ USERFUNKTIONEN ON

Når userfunktionen er on udskrives der via userfunktionen i NAS-SYS, det vil sige den udskriftsrutine hvis adresse ligger i $UOUT (0C78H-0C79H). Denne rutine bør følge de regler, der står beskrevet i afsnittet INPUT AND OUTPUT i NAS-SYS manualen.

U- USERFUNKTIONEN OFF

Fjerner userfunktionen.

W VARMSTART NAP

Først undersøges om NAP ligger i RAM (1000H til 1FFFH) i systemet. Hvis dette er tilfældet hoppes der til 1002H; ellers hoppes der til D002H. Hvis NAP ikke er indlæst bør denne kommando undgås.

X NULSTIL OPTIONS

Nulstiller alle options ("C","L","R" og "U"), undtaget hexnotation ("H"), der bliver sat on.

= aa bb cc dd DISASSEMBLER DIREKTE

Denne kommando disassemblerer og udskriver instruktionen givet ved aa bb cc dd. Eksempelvis vil kommandoen "=21 40 5" udskrive "LD HL,0540H". Det er ikke nødvendigt at indtaste alle 4 tal men kun det antal, der berører instruktionen.

ULOVLIGE INSTRUKTIONER:

I Z-80 maskinkode kan der forekomme ulovlige instruktioner, det vil sige instruktioner, der ikke forstås af processoren. Hvis en sådan mødes, bliver den første byte byte af instruktionen udskrevet, som om den var data (dvs. med en DB pseudoinstruktion), hvorefter NIP fortsætter disassembleringen fra næste byte. For eksempel vil den ulovlige instruktion ED 00 blive disassembleret til:

```
1000 ED          DB   EDH
1001 00          NOP
```

APPENDIX A -- FEJLMEDDELELSER:

ERROR 00 FORKERT KOMMANDOLINIE

Kommandolinien starter med en ukendt kommando, eller de tal, der efterfølger kommandoen, er uforståelige eller ulovlige.

ERROR 01 DATAOMRÅDEBUFFEREN ER FULD

Der er plads til 2 x 48 adresser i dataområde-bufferen.

ERROR 02 NAP TEKSTBUFFEREN ER FULD

Svarer til ERROR 99 i NAP.

ERROR 03 SYMBOLSTACKEN ER FULD

ERROR 04 KOMMANDOFEJL

Den pågældende kommando blev efterfulgt af for få tal.

ERROR 05 SYMBOLSTACK IKKE DEFINERET

Symbolstackens start- og slutadresser skal defineres (med "S" kommandoen) før labelfunktionen tages i brug.

APPENDIX B -- NIP ADRESSER:

NIP ligger i lageret fra 2000H til 2B80H (C400H til CF80H for ROM versionen), og bruger fra 0E00H til 0F00H som arbejdslager. Desuden benyttes lageret fra 0F00H til 1000H tilfælles med NAP til stackpointer og tekstbuffere. I arbejdslageret kan følgende adresser være af interesse for brugeren:

0E00-0E01	Næste ledige adresse i dataområdebufferen
0E02-0E03	Symbolstackens slutadresse
0E04-0E05	Symbolstackens startadresse
0E06-0E07	Offset
0E08	Flags
0E09-0EFF	Dataområdebuffer
	0E09-0E0A Startadresse på første område.
	0E0B-0E0C Slutadresse på første område.
	0E0D Første områdes dataformat.
	0E0E-0E0F Startadresse på andet område.
	0E10-0E11 Slutadresse på andet område.
	0E12 Andet områdes dataformat.
	etc....

APPENDIX C -- KOMMANDOOVERSIGT:

A xxxx yyyy z	Definer dataområde
B xxxx yyyy	NAP tekstbuffer adresser
C+	Comments on
C-	Comments off
D xxxx yyyy zz	Disassemblering
E	Slet dataområde adresser
F xxxx yyyy ..	Find søgestreng
H+	Hexnotation on
H-	Hexnotation off
J xxxx	Disassemblering med jumptest
L+	Labels on
L-	Labels off
O xxxx yyyy	Definer offset
Q	Quit
R+	PCR-funktion on
R-	PCR-funktion off
S xxxx yyyy	Symbolstack adresser
T xxxx yyyy zz	Tabuler
U+	Userfunktion on
U-	Userfunktion off
W	Varmstart NAP
X	Nulstil options
= aa bb cc dd	Disassembler direkte